The Center on Terrorism and Irregular Warfare

The Future of Armed Resistance: Cyberterror? Mass Destruction?

Final Report

on
a Conference Held May 15-17, 2000
at the
University Pantheon-Assas (Paris II)

David Tucker
Associate Professor

Monterey, California
September, 2000

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2000		**00-00-2000 to 00-00-2000**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Future of Armed Resistance: Cyberterror? Mass Destruction?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Center of Terrorism and Irregular Warfare,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Center of Terrorism and Irregular Warfare, Held on 15-17 May 2000 at the University Pantheon-Assas (Paris II)

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**25**	

Executive Summary

In May, 2000, a conference convened to examine the decisionmaking process that leads sub-state groups engaged in armed resistance to develop new operational methods. The conference was particularly concerned to understand whether such groups would engage in cyberterrorism, including the conditions under which they might try to cause mass disruption of information systems. The conference also examined whether such groups would try to cause mass casualties, particularly through the use of chemical, biological, radiological or nuclear (CBRN) weapons.

The conference, organized by the Center on Terrorism and Irregular Warfare of the Naval Postgraduate School, with the assistance of the Centre de Recherche sur les Menaces Criminelles Contemporaines of the University of Paris (II), was unprecedented in that its participants included former and active members of terrorist groups, as well as a hacker. It was equally unprecedented in the amount of time within and outside the formal structure of the conference that investigators were able to spend with these unique participants and in the opportunity to work with them through a series of problems in a controlled simulation. Together these characteristics made the conference an unique opportunity to learn about terrorism.

The conference reached five principle conclusions:

1. The practitioners in the conference did not use information technology to cause mass disruption. They sought to inflict mass casualties only in one narrowly defined situation.

2. Because sub-state groups with political objectives have reasons to limit the casualties they cause, these groups may find cyberterror an attractive non-lethal weapon.

3. By making it easier for sub-state groups to get their message out, the information and communication revolution may lessen the need for violence.

4. Judging from the small sample represented at the conference, terrorists have not yet integrated information technology into their strategy and tactics.

5. Again based on the small sample represented at the conference, significant barriers between hackers and terrorists may prevent their integration in one group.

6. Although sub-state groups with political objectives have strong incentives not to use force indiscriminately and to avoid attacks that cause mass casualties, a politically motivated group can find itself in a situation where its weakness and isolation make a mass casualty attack a rational choice.

Fuller statements of these conclusions are set off in highlighted boxes in the body of the report for easy reference.

This report details the reasoning that leads to these conclusions. It also explains how they confirm or amend previous research on cyberterrorism. Finally, the report offers an assessment of innovation in terrorist groups, developing a better profile of which kinds of groups will be innovative and under what circumstances. This is an issue essential to any effort to determine which groups under which circumstances might turn to cyberterrorism and mass casualty attacks. The report also contains a transcript of the conference (Appendix A).

The Future of Armed Resistance: Cyberterror? Mass Casualties?

Final Report

on
a Conference Held May 15-17, 2000
at the
University Pantheon-Assas (Paris II)

Introduction

In May, 2000, a conference convened to examine the decisionmaking process that leads sub-state groups engaged in armed resistance to develop new operational methods.[1] The conference was particularly concerned to understand whether such groups would engage in cyberterrorism,[2] including the conditions under which they might try to cause mass disruption of information systems. The conference also examined whether such groups would try to cause mass casualties, particularly through the use of chemical, biological, radiological or nuclear (CBRN) weapons.

The conference was unprecedented in that its participants included former and active members of terrorist groups, as well as a hacker. It was equally unprecedented in the amount of time within and outside the formal structure of the conference that investigators were able to spend with these unique participants and in the opportunity to work with them through a series of problems in a controlled simulation. Together these characteristics made the conference an unique opportunity to learn about terrorism.

This report first describes the participants in the conference and its structure and then the conference results. It follows this section with a discussion of the degree to which the results of the conference can be trusted, given the unique character of its participants. The report concludes with some suggestions for further research. Appendix A contains a transcript of the conference. Appendix B contains excerpts from *Cyberterrorism, Prospects and Implications*,[3] a previous report of the Center on Terrorism and Irregular Warfare. These excerpts will assist the reader in understanding the results of the conference and how they modify two conclusions of

[1] The conference was organized by the Center on Terrorism and Irregular Warfare of the Naval Postgraduate School, with the assistance of the Centre de Recherche sur les Menaces Criminelles Contemporaines of the University Pantheon-Assas (Paris II).
[2] Cyberterrorism is the unlawful destruction or disruption of digital property in order to intimidate or coerce governments or societies in pursuit of goals that are political, religious or ideological. For a fuller discussion, see *Cyberterror, Prospects and Implications*, Center on Terrorism and Irregular Warfare (Monterey, California: July, 1999), pp. 7-18.
[3] See the reference in footnote 2 above.

the earlier study. Appendix C provides information that was given to participants at the beginning of the simulation.

Participants and Structure

Five individuals with experience in violent sub-state groups plus a hacker (hereafter referred to as practitioners) participated in the conference. One practitioner came from the PLO (currently serving in the Palestinian Authority); two from the Basque Fatherland and Liberty-Political/Military (ETA-PM); one from the Liberation Tigers of Tamil Eelam (LTTE); and one from the Revolutionary Armed Forces of Colombia (FARC). All of the practitioners who were or are members of organizations had or have decisionmaking roles in those organizations. The hacker had substantial experience attacking information systems. These practitioners were joined by 11 academics, including several of the leading authorities on terrorism, and a UN official, who has done extensive research on suicide bombing in the Middle East.

All discussions at the conference were conducted under a provision of non-attribution. Comments made at the conference may be used but without attributing them to any participant.

During the first day of the conference, four academics and two practitioners made presentations. Each presentation was followed by discussion.

Academic	"Innovation in Strategies of Conflict"
PLO-PA	"Dismantling the Abu Nidal Organization"
Academic	"To Escalate or Not to Escalate? Factors Determining Insurgent Group Decisions to Increase the level of Violence"
Academic	"Bonding and Discipline in Direct Action Units: A Cross-Cultural Inquiry"
ETA-PM	"The Decision of ETA-PM to Halt Violence"
Academic	"The Effect of Government Responses to an Insurgency"

During the second day of the conference, the organizers split the participants into three groups for a simulation based on the current situation in Chechnya. One group was the Chechen resistance in Chechnya, the second was a group of Chechens and sympathizers based in Moscow and the third was a control team that played the Russian government, the rest of the world and, for the Chechen team based in Chechnya, a Moscow Chechen resistance cell. An academic chaired the Chechen team based in Chechnya, which also included the two former ETA-PM members, the FARC representative and the hacker. The PLO-PA representative chaired the Chechen group based in Moscow, which also contained the former LTTE member. The two Chechen groups were asked to develop strategies based on their situations and resources. The simulation was played in three sessions. In the first, the two groups were allowed to develop their strategies without interference or provocation from the control group. In response to these strategies, the control group increased the pressure in each of the succeeding two sessions and, in the last session, introduced the possibility of using a chemical weapon. Pressure on the groups

was increased by telling them, for example, that world opinion was largely indifferent to their struggle, that there was a media blackout imposed by the Russians, and that the Russians had begun to deport Chechens and resettle Russians in Chechnya. One of the groups was given the opportunity to use information technology in the second session of the simulation. The simulation was structured in this way to see what the participants would do on their own and then to see how far they would escalate under increasing pressure and provocation.

The third day of the conference began with the teams preparing reports on lessons learned from the simulation. These reports were then presented to a plenary session of the participants and discussed. The conference concluded with some final remarks from one of the ETA-PM members on the closing down of that group's operations.

Results

The papers presented at the conference, the discussions that occurred throughout its three days and, above all, the simulation led to important results concerning the likelihood of mass disruption and mass casualty attacks. They also suggested a number of other important findings about cyberterrorism. We present the mass casulaty and cyberterrorism results first (1-5 below) and then mass casualties (6 below).

1. The practitioners in the conference did not use information technology to cause mass disruption. The reasoning and approach of the practioners throughout the conference supported the conventional wisdom that politically motivated terrorists have reasons to target selectively and to limit the effects of their operations.

2. Because sub-state groups with political objectives have reasons to limit the casualties they cause, these groups may find cyberterror an attractive non-lethal weapon.

3. By making it easier for sub-state groups to get their message out, the information and communication revolution may lessen the need for violence.

4. Judging from the small sample represented at the conference, terrorists have not yet integrated information technology into their strategy and tactics.

5. Again based on the small sample represented at the conference, significant barriers between hackers and terrorists may prevent their integration in one group.

6. Although sub-state groups with political objectives have strong incentives not to use force indiscriminately and to avoid attacks that cause mass casualties, a politically motivated group can find itself in a situation where its weakness and isolation make a mass casualty attack a rational choice.

We will discuss each of these conclusions in turn. Summary statements of them can be found at the end of each of the following sections in highlighted boxes.

1. Causing Mass Disruption Is not a Useful Tactic

During the simulation, one of the practitioners commented repeatedly that his goal was not just to kill people but to create fear, panic and chaos (pp. 77, 78, 85, 86, 89, 91).[4] It was not violence that he cared about, as much as the psychological reaction to it. This was the best way to get attention for his cause. This approach suggests that politically motivated terrorists might want to use information technology to cause mass disruption, since this would appear to be a good way to cause fear and panic. The simulation at the conference suggested several reasons why this would not be the case. One of the simulation groups authorized an attack on the Russian Stock Exchange. This attack initially created the sentiment in the group that they might have gone too far and risked creating a backlash. Ultimately, especially after one practitioner pointed out the benefits of the attack and placed it in the context of their situation, they decided they had not (p. 62). But if an attack on one stock exchange created this fear of a backlash or loss of legitimacy, then an effort at mass disruption would seem even more likely to and thus not be acceptable. In addition, agreement to authorize the attack was based on the understanding that participation in the stock exchange was an elite activity and thus that disrupting it would not affect most Russians (pp. 59, 61). The attack was appealing, then, because it was carefully targeted at a small segment of the Russian population, an attack on which might be popular with Russians at large. Mass disruption would be contrary to this reasoning. Also, the practitioner who argued that the attack was a success was from the most ideologically anti-capitalist group represented at the conference. He liked the attack on the stock exchange for its symbolic value. While mass disruption would obviously attack e-commerce, it would also strike at many organizations sympathetic to at least some of the goals of the anti-capitalist group, if not the means it was using to achieve them. In sum, mass disruption appears to be too indiscriminate for politically motivated groups. Finally, as we will discuss in detail below, one of the principal appeals of information technology to politically motivated terrorists is the powerful assistance it provides for getting their message out. These terrorists are likely to think twice about attempting mass disruption, then, since it could make the vital task of informing the world more difficult.

> Mass disruption is not well suited to the objectives or operational approach of politically motivated terrorists. They will have good reasons not to engage in such attacks and to prefer more focused and selective attacks on information targets.

2. Cyberterror May Be an Attractive Non-Lethal Weapon

In order to understand why terrorist groups with political objectives may find cyberterror an attractive non-lethal weapon, we must consider why such groups want to limit the amount of bloodshed they cause. The conventional wisdom about terrorists with political objectives is that they use violence as a way of getting attention, not as an end in itself. This idea is neatly

[4] Unless otherwise noted, page number references in the text are to the transcript of the conference in Appendix A.

expressed in Brian Jenkins' often quoted aphorism that "terrorists want a lot of people watching and a lot of people listening and not a lot of people dead."[5] The reason that terrorists want attention and not deaths is that their undertaking is a political one. They want an audience to listen to their claims and demands and, in the best case, to become sympathetic to them. Terrorist violence, of course, has an undeniably coercive component. It is meant to instill fear and to intimidate. But this violence can go too far. Too much violence, too many deaths or too many of the wrong kind (children, for example), risks alienating any possible sympathizers and making any level of action against the terrorists seem justified. Underlying these calculations about the effective level of violence is an understanding of the common revulsion at wanton killing. If a group and its political objectives are to have any chance of acquiring and maintaining legitimacy in the eyes of the world at large, it must not appear to kill wantonly. Its use of violence must be proportionate to some threat.

This reasoning does not necessarily lead to the conclusion that politically motivated terrorist violence will be small-scale. If the threat is great, the violence could be great. One of the former members of ETA-PM argued at the conference, for example, that the repression of the Franco government was so great and posed such a threat to the Basque people that they could tolerate a lot of violence being done in their name (p. 24). In at least one interview, Osama bin Ladin seemed to argue that he was justified in using weapons of mass destruction against Americans because this was a proportionate response to the threat that the United States posed to Islam and the Holy Land.[6] In addition, a terrorist group can undertake by itself or through a political apparatus a public information campaign to make the public more accepting of violence against the state and its representatives and institutions. ETA did this as it escalated its attacks, according to one former member (p. 23). It is also possible that a terrorist organization could mistake what public opinion will tolerate. It might think that its public audience would accept a certain level of violence, perpetrate an attack that produces it and then find out it was wrong. If it makes this mistake, an organization is likely to lose support.[7] As a participant in the conference made clear, ETA split in the early 1980s over such judgments about public opinion (p. 33-34). Again, over time an organization might become less concerned with winning over public opinion and rely solely on coercion and intimidation to maintain the minimum level of support necessary to conduct its operations. While at this point functioning like a criminal enterprise rather than a terrorist group, such an organization might be willing to commit extreme forms of violence. For these reasons, the conventional wisdom about terrorist groups with political objectives does not mean that the violence they produce will always be small-scale. Yet, the critical point in the conventional wisdom is still valid: any group that seeks to build legitimacy or public support must commit acts of violence that the public perceives to be proportionate and justifiable.

---

[5] On the conventional wisdom and some reasons why it may no longer apply, see Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), pp. 198-205.

[6] Jamal Ismail, "I Am Not Afraid of Death," *Newsweek*, January 11, 1999, p. 37. Consider also the discussion of bin Ladin in the conference, Transcript, p. 18.

[7] This appears to have happened to Islamic terrorists in Algeria and Egypt. See Fawaz A. Gerges, "The Decline of Revolutionary Islam in Algeria and Egypt," *Survival* 41 (Spring, 1999), 113-125

Substantiating this line of reasoning is the fact that the practitioners at the conference used the term "terrorist" to describe only those who killed indiscriminately (cf. pp. 9 and 105). Their more measured use of violence fell below that threshold. They used only that level of violence necessary to make their cause known and to increase the pressure to meet their demands, without ultimately endangering the legitimacy of those demands. (Consider the comments of the practitioners on pp. 14, 50, 60, 64, 73, 78-79, 89-90, 104). This supports the argument that those who participate in sub-state groups that use political violence see it as an instrument rather than an end in itself and use it according to some rules of proportionality.

The courses of action developed in the simulations at the conference further support this line of argument. With one important exception (discussed below, pp.16-18), in keeping with their experience in nationalist and revolutionary movements and the circumstances of the scenario, the practitioners treated violence as instrumental. They insisted that the struggles they had been involved in and the one presented in the scenario were above all political struggles (e.g., p. 59). All efforts, including all uses of violence, had to be subordinated to the political objective of the struggle. This meant that the ultimate objective was to win domestic and international support. This meant, in turn, close and constant attention to public and international opinion. Violence was acceptable if it could be made to appear legitimate, that is, if it was proportionate, for example, to the level of perceived repression (pp. 66-67, 92, 105-106). The assumption was that this proportionate use of violence would win more public support or attention than it lost. Thus, both of the Chechen groups in the simulation initially targeted government officials, arguing that this was a better tactic than killing the public indiscriminately (p. 54-55, 70-71). Among government officials, both groups tended at first to agree that targeting corrupt officials or those plausibly associated with human rights violations was a better tactic than killing government officials indiscriminately (pp. 50, 70). In this light, it was interesting that a relatively old-fashioned tactic, kidnapping, received support in both groups and particularly the one based in Chechnya. One practitioner in this group appeared to be following the logic of the conventional wisdom when he argued that a kidnapping was better than a bombing because a kidnapping lasts longer, produces more publicity, and creates the possibility of negotiations, which confer legitimacy on the sub-state group, while keeping violence to a minimum. The hostage, he informed the group, could always be released unharmed (p. 65).

The conference, then, confirmed the conventional wisdom about violent sub-state groups with political objectives. Such groups want people paying attention and not dead. For this reason, cyberterror may be an attractive non-lethal weapon. In the simulation, the group based in Chechnya wanted to use information technology to attack infrastructure, as a way of dramatizing its message without killing people. A noted above, it was able to use such technology to shut down the Russian stock market.[8] When they were told that this act had caused great concern in Russia and in political and financial capitals around the world, the group concluded that this action had been a great success (p. 62). It got them attention but did not cause concern about

[8] The group was told that members of the Chechen diaspora in the Middle East had offered through reliable intermediaries to attack the Russian Stock Exchange and the Ministry of Defense.

fatalities or casualties inflicted. It appeared to provide significant political benefits, then, without threatening high political costs.

With this line of reasoning in mind we should recall the comments of the practitioner mentioned above. If it is not violence but the psychological reaction that is important to a terrorist, then cyberterrorism should be deemed a useful tool. Mass disruption might be too indiscriminate but more selective attacks should still be useful. They could generate panic without causing bloodshed and so limit any possible backlash.

We should note, however, that as with traditional kinds of terrorist attacks, reasons for restraint with information attacks do not mean that terrorists will always be selective in their targetting or choose small-scale targets. As discussed above, extreme repression, miscalculation or transformation into a criminal enterprise might lead even nationalist or revolutionary groups to undertake larger-scale attacks. Generally speaking, however, groups with political motivations will have reasons to target selectively and not engage in mass disruption.

Cyberterror will also appeal to groups, the simulation suggested, because it will keep operational as well as political costs low. All of the practitioners at the conference were more aware than the academics of the costs of undertaking clandestine violent activity. This was most apparent in the Moscow group, which was under the most pressure. Both practitioners continually pointed out to the academics the difficulties and dangers involved in what they were proposing to do: suicide bombing might be an effective tactic but it is hard to find people willing to do it and requires more complicated logistics; if members of the Moscow group carry out suicide attacks, trained and trusted personnel would be lost without any guarantee that they could be replaced (p. 75, 91, 99-100); hostage-taking may be a useful tactic but imposes significant operational requirements on the group undertaking it (p. 98); surveillance consumes vast amounts of time and personnel (pp. 7, 83); LAWs and stingers can be effective weapons but transporting them in a city as tightly controlled as Moscow will likely lead to arrests rather than effective operations (p. 99); simultaneous operations might be more attention-getting but they are extremely difficult to coordinate (p.81). In short, the practitioners were acutely conscious of the costs of conducting operations. Anything that can lower those costs, therefore, should recommend itself to them. Information technology offers that possibility. It can be used remotely, thus lowering the cost of maintaining security. Surveillance on the web can be automated to some extent, saving personnel costs, and done anonymously, lowering security costs. The materiel needed is small and easily transported, which lowers financial and security costs. For clandestine sub-state groups, which are chronically short of resources and vitally concerned with security, information technology would appear to offer significant advantages.

A previous report on cyberterrorism, *Cyberterror, Prospects and Implications* (hereafter CPI), reached some conclusions similar to those drawn from the conference. For example, CPI also concluded that politically motivated terrorists would be unlikely to engage in mass disruption (CPI, pp. 49, 52). The conference results also confirm other conclusions that this

report reached about the kinds of terrorists at the conference (ethno-nationalist separatists and revolutionaries).[9] As the analysis has indicated so far, it confirms that

1. Attacks on infrastructure appeal to politically motivated terrorists (CPI, p. 45);
2. Cyberterrorism would allow terrorists to gain publicity without alienating supporters with excessive violence but the unintended effects of cyber attacks might discourage groups from using them (CPI, p. 47);
3. Revolutionary or anti-capitalist terrorists would use cyberterrorism for focused attacks on governments and corporations (CPI, p. 52).

About point two above it should be noted that, at least based on the sample attending the conference, thinking about the use of information technology among terrorists has not advanced far enough so that their calculations about the utility of cyberterrorism sufficiently take into account unintended consequences. This is an issue to which we return below.

In addition to the three conclusions listed above, CPI reached two other conclusions concerning politically motivated terrorists. It concluded that

4. Given the costs of acquiring a sound technical capability, groups operating within a disputed territory would probably stay with traditional terrorist operations, while those operating outside the disputed territory would be more likely to use cyberterrorism to launch attacks into the disputed territory and against "the critical infrastructure of international supporters of the incumbent regime (when the selected targets are not in the immediate area of operations, cyberterror attacks offer reduced vulnerability and potentially more efficient use of resources") (CPI, p.46);
5. A group operating in a country with minimal dependence on information systems and limited connectivity would find cyberterrorism less attractive (CPI, p.48);

As the analysis so far has made clear, the results of the conference suggest that these conclusions need to be amended.

Point four is that the costs of acquiring more than a rudimentary cyberterrorism capability might encourage groups to remain with traditional terrorist techniques when operating domestically, while using cyberterrorism internationally. This preference for using cyberterrorism for international attacks derives from the presumed higher costs of these attacks (organizing and supporting attacks from overseas is more difficult, perhaps impossibly more difficult, than organizing and supporting them locally), which would make the investment to have this capability a reasonable one. While the simulation gave the participants the capability to use or authorize the use of information technology for free, and thus cannot offer a definitive assessment of what terrorists would be willing to pay for what degree of this capability, the

[9] Since ethno-nationalist and revolutionary terrorists were the only kind present at the conference, its results do not apply to the other kinds of terrorists discussed in CPI: far right extremists or religious or New Age terrorists. Questions about these groups can be addressed only by further research. See Suggestions for Further Research below.

earlier report probably failed to assess fully the costs to terrorists of traditional techniques, that is, of operating without information technology. In other words, sitting with the practitioners and listening to them work through operational problems highlighted their concern with the costs of traditional terrorist activities. These costs are so high from the perspective of the terrorists that they should be willing to invest significantly in technologies and expertise that would lower them, especially for their domestic operations, where at least security costs are likely to be higher than for international operations. Terrorist groups may be even more likely to make this investment because, as noted above, the conference suggested they will not need to have the greatest and most expensive cyberterror capability (what the earlier report called a complex-coordinated capability),[10] which would allow them to cause mass disruption. Instead, they are likely to be satisfied with an advanced-structured capability, which "is the level where cyberterror attack becomes realistic as a primary method of attack." (CPI, p. 81) As with any investment in new technology, investing in cyberterrorism would be a gamble but, given its potentially great benefits, one that terrorists may well be willing to make. Even acquiring rudimentary capabilities for attack might be appealing, although as CPI made clear (CPI, p. 47) such capabilities can be easily countered and may not rise above the noise level of non-terrorist hacker activity.

Point five is that cyberterrorism will be less attractive in countries with less connectivity and dependence on information systems. This proved not to be the case in the simulation. Saying that a country is not dependent on information systems or well-connected is tantamount to saying that cyber activity in that country is an elite phenomenon. As an elite phenomenon, it is an attractive target to any group trying to build broad popular support. Attacking the elite will not effect the mass of people and may even be popular with the mass. As noted previously, these assumptions lay behind the attack on the Russian Stock Exchange in the simulation. Furthermore, the lack of connectivity in a country serves to insulate people from the unintended consequences of a cyber attack. Since, as noted above, CPI offered these unintended consequences as something that might discourage terrorists from using information technology in their attacks, limited dependence on information systems and low rates of connectivity might actually encourage cyber attacks rather than discourage them.

The utility of cyberterror as a non-lethal weapon was highlighted by the FARC member in his comments in the after-action session on the simulation. "Through a friendly hacker we were able to bring down the information technology at the Moscow stock exchange. It had to stop work for one day and this had an enormous effect outside Russia. So any attack using the techniques of the hackers could be extremely useful" (p. 104).

[10] Appendix B contains excerpts from *Cyberterror, Prospects and Implications* defining these levels of capability.

The conference results suggest that ethno-nationalist and revolutionary terrorist groups will find cyberterrorism appealing as a non-lethal weapon because it will allow them to achieve their objective (more attention to their cause) while lowering their political and operational costs. Amending earlier work on cyberterrorism, the conference results also suggest that an array of groups (both the resource poor and rich) in a variety of situations (operating domestically as well as internationally, in countries of low connectivity and high) could find cyberterrorism useful.

3. Information Technology May Lessen the Need for Violence

The discussion of information technology has so far focused on its use as a non-lethal weapon. The conference also highlighted the importance of information technology as a means of communicating a message. This aspect is arguably more important than the use of cyberterrorism as a non-lethal weapon, since for terrorists with political objectives, violence is ultimately only a means to get attention for the cause.

In his presentation to the conference on the first day, one of the ETA-PM practitioners argued that the new information technology meant that violence was less important than it had been in the past (p. 23). The purpose of violence was to get attention but this could now be done more effectively than in the past through new information and communication technology, which governments could not control. As non-violent means of propagating the message increased, the need for violent means decreased. In the simulation, when informed by the control team that the Russians had removed all foreign media from Chechnya, this practitioner was not concerned. Chechen web pages in the Middle East and Europe, e-mail, and video footage would get the story out and, he was convinced, the Russians could not prevent this. Other members of this group called for better information campaigns and similarly assumed that they could communicate with their intended audience (pp. 62-64).

There are limits to this argument. Putting information in front of people does not mean that they will pay attention to it. Violence forces people and governments to pay attention and respond. Ibrahim Rugova pled the Kosovars case non-violently but the international community did nothing. When the Kosovo Liberation Army began its attacks and the Serbs responded, the international community got involved.[11] More web pages, e-mails or video footage or their more savvy use might have garnered Rugova more support but this is far from certain. The Zapatistas are generally considered sophisticated users of the new media and this has gotten them support. Yet, they have used force and military trappings as part of their campaign and their international support has not really spread beyond a limited circle of concerned citizens and non-governmental organizations. It has not translated into support from other governments, who apparently believe

[11] Ivo H. Daalder and Michael E. O'Hanlon, *Winning Ugly, NATO's War to Save Kosovo* (Washington: The Brookings Institution, 2000), pp. 10, 186.

that the costs of providing this support have remained higher than its perceived benefits, or given them decisive leverage against the government in Mexico City. The same would probably have been true in Kosovo, even if Rugova had run a more sophisticated information campaign.

The practitioner acknowledged these limits. He did not claim that violence would no longer be necessary. He insisted, however, that if he were building a movement today, it would require less violence than it did when he began his clandestine activities over 25 years ago. First, he mentioned the success that non-governmental organizations have had with non-violent web-based campaigns. Second, he argued that building or maintaining ethnic or national group cohesion would be easier today with modern communications and would require less violence, even in the face of an oppressive government.[12]

On balance, there is probably some merit to the practitioner's argument. Clearly, there could be a level of government repression that would nullify, if not entirely the use, then the effectiveness of the new means of communication. Just as clearly, the new means of communication allow sub-state groups to organize resources for resistance, including domestic and international public opinion, in ways that governments cannot stop.[13] It therefore seems reasonable to conclude that, in those cases where a government has reason to resist a sub-state group but either not the means or the reason to impose a maximum level of repression, the information and communication revolutions may permit the sub-state group to achieve its goals with less violence than it would have used in the absence of these revolutions.

In some circumstances (when the costs to a state of acknowledging the claims of a sub-state group are not too high), the information and communication revolutions may diminish the amount of violence necessary to mobilize sub-state resistance and achieve its objectives.

4. Terrorists Have Not Fully Integrated Information Technology into their Strategy and Tactics

The focus of the practitioners on political objectives and domestic and international opinion suggests that they would readily use information technology to further their cause. This

[12] Conference presentation (p. 23) and discussion with a member of the control team, May 15 and May 17, 2000. For the importance of group cohesion for movements of protest or rebellion, see Ted Robert Gurr, *Minorities at Risk, A Global View of Ethnopolitical Conflicts* (Washington: United States Institute of Peace, 1993), pp. 123-138, especially pp. 127-128, 131.

[13] Opposition to the government in Burma, having been chased from the cities, has organized itself in Burma and around the world from Burma's jungles thanks to modern communications. See Thomas Crampton, "Latest Technology Links Jungle Rebels, Wired Revolution Helps Guerillas," *International Herald Tribune* (October 8, 1999).

was not the case. Only the practitioner discussed in the section above displayed a consistent and thorough understanding of how information technology might be used in sub-state conflicts, and his understanding was restricted to using this technology to convey information. He did not display any understanding of how to use information technology as a weapon. The other practitioners did not display even this much knowledge of information technology or how it might be used in a sub-state conflict. When late in the scenario they were presented by the control team with the opportunity to launch cyber attacks against the Russians, the Chechen group based in Chechnya authorized the disruption of the Russian stock market, as already mentioned, and logistics data bases in the Russian Ministry of Defense. They did this, however, only after the hacker in the group reminded them that the control team had presented them with this opportunity, the hacker brought it up again and the academics urged the group to do it and an academic once again brought it up (pp. 57, 59). The practitioners agreed to the attack without the kind of detailed analysis of how best to exploit operational possibilities or without the careful consideration of consequences provoked by other suggested operations. None of the practitioners suggested, for example, that the ability to penetrate Russian information systems might be more valuable as a source of intelligence than as a weapon of disruption, even though the group had discussed previously its intelligence deficiencies and one of the practitioners had discussed using negotiations as a means of collecting intelligence (pp. 47, 49, 50, 52, 58, 60, 61). At the end of the simulation, it was an academic who was still trying to figure out new ways to use information attacks (p. 65). In general, the practitioners did not show the familiarity with the tactical possibilities or strategic consequences of information technology that they showed with bombings, kidnappings, assassinations or other traditional insurgent and terrorist tactics.

The hacker reached a similar estimation of the other practitioners at the conference. According to him, in private conversations they showed an interest in information technology as a weapon and a means of gathering or controlling information and familiarity with the possibilities of information technology beyond what the general public may have but no practical experience with it.[14]

This attitude toward information technology is consistent with a general tendency of the practitioners in the simulation not to innovate, to be conservative tactically (characteristics that confirmed hypotheses developed in the first session of the conference, pp. 2-3) and to use violence carefully and selectively. This conservative approach or reliance on traditional methods may have resulted from the fact that three of the six practitioners are retired, so to speak, and in two cases retired for almost twenty years. On the other hand, the practitioner who is still involved (the FARC representative) was no more innovative than any of the other practitioners; the PLO-PA representative, who currently works in a position that would presumably keep him aware of more recent developments, did not display a more subtle grasp of the potential of information technology; and, finally, the practitioner who displayed the greatest awareness of the utility of information technology in information campaigns was one of the long retired

[14] Conversation with one of the conference organizers, May 18, 2000.

practitioners. The conservative approach of the practitioners, therefore, may not be the result of their retired status but evidence for the claim that terrorists are tactically conservative.[15]

The conference highlighted, then, a tension or gap between the evident advantages of cyberterrorism and an equally evident tendency on the part of terrorists not to innovate. The critical question, then, is under what circumstances this gap might be bridged and cyberterrorism become a standard weapon in the repertoire of terrorists. Discussions and the simulation pointed to the following conclusions:

- All innovation is difficult and therefore rare.
- Innovations are seldom completely new departures from past experience.
- Tactical innovation probably occurs more readily than strategic innovation.
- Thus, information technology is more likely to be used to do traditional things (getting the message out or attacking a symbol of wealth and power like a stock market) in new ways (setting up a web page or shutting down an information system rather than blowing up a building), than change fundamentally the character of sub-state conflict (a new balance of violence and information manipulation).
- Opportunities for innovation in the operating environment of a sub-state group are not necessarily more important for producing innovation than the decisionmaking process within the sub-state group.
- Innovation is more likely to occur in smaller and newer organizations and under leaders who are entrepreneurial.

In citing new and smaller organizations as those most likely to innovate, the conference agreed with a conclusion of CPI (p. 72) and, as far as cyberterrorism is concerned, with what the sketchy evidence reveals.[16]

In emphasizing the importance of entrepreneurial leadership for innovation, however, the conference offered a correction to the discussion of this issue in CPI, which used the life-cycle model of organizations to understand innovation. It was the view of the conference that although newer organizations are more likely to innovate than older organizations, not all such terrorist organizations do in fact innovate. A more reliable indicator of innovation than the stage of a group's development or the opportunities in its environment, according to conference participants, is the character of its decisionmaking. The conference reached the conclusion that entrepreneurial leadership is the key to understanding terrorist innovation. Opportunities to innovate may be present and an innovation, such as cyberterrorism, may offer significant benefits, but this does not mean innovation will occur. These conditions may be necessary for

[15] Bruce Hoffman, "Responding to Terrorism Across the Technological Spectrum," in John Arquilla and David Ronfeldt, *In Athena's Camp, Preparing for Conflict in the Information Age* (Santa Monica: RAND, 1997), pp. 340-344.
[16] John Arquilla, David Ronfeldt, and Michele Zanini, "Information Age Terrorism," *Current History* 99(April, 2000), 183-185.

innovation but they are not sufficient to bring it about. An entrepreneurial leader must be present (p. 2).

The conference cited Velupillai Prabhakaran, the head of the LTTE, as an example of a entrepreneurial leader. In general, conference participants agreed that a group likely to innovate will have a leader who is very hard working, in complete control over his whole organization, accepts risk, has a lot of decisionmaking autonomy, and leads a cohesive and loyal organization (p. 7).

Some discussion at the conference focused on whether resources were important for innovation (pp. 5, 7). No definitive answer was reached on this issue but it appears unlikely that resource levels will have a decisive influence on innovation with cyberterrorism, at least among terrorists with political objectives. First, resource levels do not appear to be decisive for innovation generally.[17] Second, achieving an advanced-structured capability, which is what politically motivated terrorists seem most likely to want, is not that expensive (CPI, p. 86.).

Terrorists have not fully integrated information technology into their strategy and tactics. To the extent that they have used this technology, they have tended to use it as a better means of communicating rather than as a non-lethal weapon. They have tended to innovate with information technology tactically rather than strategically. Smaller and newer organizations but above all those with entrepreneurial leadership are likely to lead the integration of information technology into terrorist tactics.

5. Significant Barriers May Prevent the Integration Of Hackers and Terrorists

In addition to examining innovation in terrorist groups, the conference and in particular the simulation inadvertently exposed another important organizational issue relevant to cyberterrorism, whether terrorists and information technologists or hackers can work together.

One of the simulation groups brought together the hacker, the FARC representative and the two ETA-PM members. Although these four practitioners agreed in general on the critical strategic objective (acquire domestic and international legitimacy) they disagreed over tactics and had difficulty communicating, particularly in the first session. This difficulty was so great that it led to a breakdown in the group. The hacker and the terrorists were not able to work together. If this breakdown can be generalized it would have obvious consequences for the development of cyberterrorism.

[17] Stephen P. Rosen, *Winning the Next War, Innovation and the Modern Military* (Ithaca: Cornell University Press, 1991), pp. 3-4, 252.

Since the conference and simulation were not set up to explore this problem and only one hacker was present at the conference, it is impossible to make any definitive statements about why this breakdown occurred. The observations of other participants and discussions with the hacker permit some speculation.

Personality clashes were part of the problem but only part. (For evidence of a personality clash, consider the exchanges at the beginning of the simulation between the hacker and the academic serving as the chairman of simulation group A, pp. 44-45). As presentations and discussions at the conference suggested, this may have been in part a question of status (p. 28). The hacker was there as a practitioner but his standing as a practitioner was probably in doubt from the viewpoint of the other practitioners. What status or standing does a manipulator of bytes at a remote and safe distance have in front of men who have planned and ordered bombings and killings and lived clandestine lives under the threat of torture and death (pp. 33, 78, 82)? To conduct cyberterrorism effectively, groups will need educated information technology specialists. Such a degree of education would normally provide someone a significant status. If that status is not accorded to these information technologists by terrorist groups, will they remain in these groups or function well in them?

The differences between the hacker and the practitioners went beyond issues of status. They disagreed over tactics. The practitioners quickly turned to the issue of how to use violence and whom to target. The hacker's approach was to look first at the opportunities for getting the group's message out and how those opportunities might be increased. The hacker did not oppose the practitioners' use of selective violence, while the practitioners for their part agreed that getting their message out was critical. The difference between the two was over tactical emphasis or priorities and the way this different emphasis was expressed. The hacker spoke in theoretical terms compared to the more direct speech of the other practitioners. (Again, consider the exchange between the chairman and the hacker, p. 45). The hacker spoke about the need to establish a social contract between the insurgents and the population they sought to represent, for example, while the practitioners spoke about the connection to this population not as something to be crafted or won but as a given. Accepting it as given, the practitioners tended to turn quickly to political requirements or activities, for example the need to set up an Army to show that their insurgent movement was a functioning state. The practitioners, it emerged, agreed that the loyalty of the people had to be maintained but they spoke about this task in what might be described as more operational terms (setting up an Army, establishing authority over a territory) (pp. 48, 53). This difference in approach was not just a matter of the words used but appeared to be part of a different conception of the problem at hand. The practitioners' approach was keyed more to typical political considerations than was the hacker's. The hacker, more than the practitioners, appeared to want to clarify the political framework first and then address specific problems.

By the hacker's own assessment, the disagreement over tactics was in part based on a different approach to conceptualizing problems. When the group was discussing attacking oil pipelines, everyone, including the hacker, talked about bombing it. But the hacker moved from this approach to discussing the pipeline as an information system (cf. pp. 58 and 59). It could be

shutdown, he proposed, by attacking its control system. This suggestion was not taken up by the other practitioners, evidence to the hacker that they did not see that the world was really composed of systems and networks and that understanding these was essential.[18]

Finally, although this did not come up explicitly during the conference, the hacker agreed that his interaction with the traditional practitioners pointed to potential organizational problems for any hacker-terrorist collaboration. On those occasions when they do not operate alone, hackers operate in flat open-ended associations, while terrorists have often operated in closed hierarchical organizations. It is an open question whether these two organizational styles, developed in different operational environments and derived perhaps from different psychological needs, can be brought together. One of the former ETA-PM members stressed in his remarks the need to belong and the strength of attachment to the group as characteristic of those in clandestine organizations (pp. 33, 106). These are not necessarily character traits typically associated with hackers. Assuming that they see sufficient benefit in working together, could the two kinds of practitioners blend their organizational styles or wholly adopt the style of the other?

The hacker believed that the problems outlined here would arise not only if terrorists tried to bring into their organization external hacking talent but even if they tried to develop that talent internally. In effect, his view is that significant hacking talent is not the result of training alone but of psychological and intellectual dispositions that if nurtured in an individual in a terrorist group would be likely to alienate that individual from the group.

If this encounter at the conference between a hacker and more traditional practitioners is at all indicative of general tendencies, it suggests that hackers will have trouble fitting into groups of traditional practitioners for psychological, tactical, and organizational reasons.

6. Political Objectives and Mass Casualties, the Conventional Wisdom and a Special Case

The focus on political objectives and legitimacy of the practitioners made CBRN weapons unattractive, as the conventional wisdom about politically motivated terrorists predicts. None of the practitioners or other participants brought up the use of these weapons on their own during the conference. Only when the control team introduced them to the groups in the simulation were they discussed.[19] The Chechen group in Chechnya consistently refused to have

[18] The hacker maintained that he was unusual in his understanding of the networked and system character of the world. This understanding was one thing that distinguished him from the typical hacker who runs downloaded hacker tools at various targets without understanding the systems he is attacking. To distinguish himself from these typical hackers, he referred to himself as an infrastructural warfare specialist.

[19] Means of inflicting mass casualties and of causing cyber damage were supplied to the groups for free on the assumption that if the utility of such means appeared great, groups would have a strong incentive to overcome

anything to do with them, no matter how adverse the group's circumstances became, for fear that it would destroy popular support and international legitimacy (p. 62). Some analysts have speculated that insurgent groups might want to possess CBRN "to strengthen a contested claim to sovereignty by taking on some of the trappings of a state."[20] Although the Chechen group in Chechnya continually sought to establish its legitimacy, it did not see the possession of CBRN as helpful in this regard. On the contrary, all members of the group agreed that the possession of such weapons would put an end to their hope of establishing Chechnya as a legitimate and independent state.

An important qualification to these generalizations about the instrumental character of violence developed rather quickly in the Chechen group based in Moscow. Initial discussions in this group followed the logic of the conventional wisdom, with one academic and one practitioner paying particular attention to public opinion. At this stage, the group was selective in its use of violence. It decided not to target non-combatants, for example, focusing instead on the Russian military or officials who were involved in the Chechen war. When at this stage it sought wider effects, it considered sabotage, including attacks on the electrical system and the subway in Moscow (pp. 70-71, 81). Soon, however, the group's concern with its audience diminished, with only the academic consistently reminding the group throughout the simulation that it should not forget the effect of its actions on Russian and international opinion. As the group's concern with public opinion diminished, its willingness to use force increased. By the end of the simulation, the Moscow group was using violence even though there was no hope that it would help it achieve its political objective (pp. 98-101). Violence had become an end in itself. It was no longer merely instrumental. It was in this context that the group agreed to use a chemical weapon (nerve gas) to inflict mass casualties.

By their own account, the Moscow group tended toward violence, ultimately extreme violence, because it was the only tool it had. The scenario put them in a situation in which they could not affect public opinion, everything else they did failed, and the control team had told them that they were about to be arrested. As one participant put it, the group's weakness bred extremism (p. 102). More important, this extremism seemed justified because of what the Russians were doing. The Russians were increasing the pressure on the Chechen population, deporting them, shooting those who resisted and importing Russians to replace them in Chechnya. This action by the Russians was taken by the group to be an assault on the Chechen nation, an effort, reminiscent of Stalin's deportation, to destroy the Chechens, a final solution to Russia's Chechen problem. A consensus developed in the group that this was an act of genocide. As such, and given the failure of all other efforts, inflicting mass casualties seemed justified (pp. 89, 93, 106).

Two different interpretations of this decision are possible. First, it could be seen as a continuation of the logic behind the conventional wisdom. This logic calls for proportionate

---

resource barriers to acquire them. These barriers are significant, of course, and no final estimation of utility in possessing or using these weapons can be made without taking them into account.

[20] Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer, *America's Achille's Heel, Nuclear, Biological and Chemical Terrorism and Covert Attack*, (Cambridge: MIT Press, 1998), pp. 207-210.

violence and that was what the group, in so far as it was able, engaged in. With a line of reasoning similar to bin Ladin's, the group argued that the Russians were destroying the Chechen nation and thus it was a proportionate use of violence to kill as many Russians as possible.

While plausible, this interpretation is ultimately not satisfactory. The group decided on the gas attack even though it expected that it would provoke even more violence against Chechens. Nor was the group dissuaded from this course of action by the acknowledged likelihood that it would destroy sympathy for the Chechen cause in Russia, if any remnant existed there, and around the world. By this point in the simulation, the group believed that the Russians were in effect trying to exterminate the Chechen people, if not every single Chechen, and that they had been abandoned by the international community. In this situation, in their own estimation, most importantly, they had passed beyond a rational calculation of tit-for-tat proportionality (pp. 98, 100).

The second interpretation of this group's use of nerve gas begins with the recognition that when all other means had failed and the threat had risen to the level of the genocide of their people and their own imminent demise what was left for this group was not terrorism as traditionally conceived but an act of revenge. As members of the group put it on two different occasions, in their self-assessment, they had nothing left to lose (pp. 92, 101-102). A rough analogy exists between the situation that the Moscow group found itself in at the end of the simulation and the situation confronted by the Jews who formed Dahm Y'Israel Nokeam (DIN) (Avenging Israel's Blood) after World War II, a group which carried out a mass poisoning of German POWs. As a recent student of this episode explains, those who carried it out were not terrorists as we normally conceive of them but members of a special category, "small radical organizations representing 'heavily brutalized communities,' or populations devastated by genocide, ethnic cleansing, or massive destruction. . . . Facing inevitable destruction or believing that life has lost all meaning, they may convince themselves that their sole possibility for self-assertion is to strike back massively against their executioners."[21] Something like this sentiment of self-assertion in the face of disaster, rather than a calculated tit-for-tat response, was behind the Moscow Chechen group's decision to use the nerve gas. Having made this decision, for example, the group speculated about whether any of its members would survive to carry on the struggle or even whether the struggle itself would continue (pp. 95, 97, 102). When the group found itself in the midst of this disastrous situation with no way out, it decided to cause mass casualties.

[21] Ehud Sprinzak and Idith Zertal, "Avenging Israel's Blood," in *Toxic Terror, Assessing Terrorist Use of Chemical and Biological Weapons*, ed. Jonathan B. Tucker (Cambridge: MIT Press, 2000), pp. 39-40.

The conference simulation supported the conventional wisdom that terrorists with political objectives will tend not to cause mass casualties but pointed to an exception, which has an analogue in the historical example of the DIN. If a population appears to be threatened with destruction, then a group affiliated with it, especially if it is isolated, failing to affect the larger struggle and is itself facing arrest or destruction, may try to inflict mass casualties using a CBRN weapon.

Why the Results are Tentative. Can They Be Trusted?

Conclusions drawn from the conference about cyberterrorism and mass casualties should be treated with caution because they are based on a small sample of practitioners. Confidence in the results should increase, however, when they are placed in the context of an ongoing research project on cyberterrorism initiated by CPI. As noted, the conference results confirmed several of the conclusions of this earlier report and amended others. In general, the conference results suggest a broader role for cyberterrorism than the earlier report did. Similarly, confidence in the conference results should increase when they are placed in the context of terrorism research generally. The conference confirmed the conventional wisdom about mass casualty attacks and modified it or highlighted its limitations through the experience of the simulation group based in Moscow. In addition, the conference refined work on innovation in terrorist groups, developing a better profile of which kinds of groups will be innovative and under what circumstances. This is an issue essential to any effort to determine which groups might turn to cyberterrorism and mass casualty attacks.

In assessing the results of the conference, it is critical to consider not only how representative were the practitioners who attended but also how truthful. Should we not assume that they were simply saying what they thought the conference sponsors wanted to hear or taking the opportunity to present their party's line and thus that the conference results are of little or no use? This question is particularly acute for the two practitioners (the FARC representative and the member of the PA), who remain engaged in ongoing political conflicts.

There was, of course, no way to be sure that the practitioners were being truthful in every utterance they made during the conference. Indeed, when given the chance to address plenary sessions of the conference, the PLO-PA and FARC representatives spent a significant portion of their time conveying the official positions of their organizations. There were, however, several ways to assess whether the practitioners were dissembling.

First, the degree of critical distance from their organizations that the practitioners displayed indicates the degree to which they were not simply espousing a party line. All the practitioners except the FARC and PLO-PA representatives displayed such distance.

Second, the practitioners comments can be gauged against the past and present actions of their organizations. The strategy that the FARC representative argued for in the simulation is identical to the strategy that the FARC is pursuing in Colombia. This increased our confidence that he was not merely telling us what he thought we wanted to hear. The PLO-PA representative was questioned closely when, in his remarks to a plenary session, he appeared to offer an account of the use of violence that did not square with past PLO practice (pp. 12-14). This resulted in a more accurate assessment of PLO-PA attitudes. This kind of assessment was done effectively because the academics at the conference had a thorough knowledge of the groups represented.

Third, the simulation imposed a set of unavoidable facts on all the participants. The responses of the practitioners were considered in the light of these facts to see if they made sense.

Finally, the conference provided a wide variety of formal and informal opportunities for discussion and assessment over a three day period. The more internally consistent the comments of a practitioner over this time, especially set against the standard of his organization's actions and the constraints of the simulation, the more confidence we can have in his veracity.

Based on these four tests, it seems fair to conclude that the comments of the practitioners were truthful and, in the case of the PLO-PA and FARC representatives, reflected the thinking of their organizations.

The comments of the practitioners shed further light on the degree to which the results of the conference can be trusted. During the group assessments of the simulation, two of the practitioners said that the simulation reproduced problems that had occurred in their experience of sub-state conflict (pp. 66, 67). One commented that what was learned in the simulation could be the basis for decisions in real life (p. 67). Yet they also pointed to a way in which a simulation is unavoidably different from reality. They insisted that their decisions to use violence selectively were rational, that is, appropriate given their objectives. They insisted equally, however, that in the world of real conflict such a rational approach could be overwhelmed by the emotions that the struggle generates. If your friends are killed by the security service, they noted, for example, the desire for revenge could overwhelm a rational approach to the use of violence (pp. 66-67, 106). Also, the struggle can come to be pursued for its own sake. The former ETA-PM member suggested that the pressures of the clandestine life forges bonds of friendship that some are reluctant to give up, even if the group appears to be achieving its objectives (p. 106, 33). In general, then, the practitioners concluded that the emotional aspects of the violent clandestine life, aspects essential to understanding this kind of life, cannot be reproduced in a simulation but that the simulation was otherwise realistic and effective.

Suggestions for Further Research

As noted in the introduction, the conference was an unprecedented opportunity to learn about terrorism and particularly the circumstances under which terrorists might use cyberterrorism or try to cause either mass disruption or mass casualties. In keeping with its unprecedented character, the conference generated intriguing insights, for example, into the potentially broad appeal of cyberterrorism as a non-lethal weapon and the possibly difficult task of combining hackers and traditional practitioners in the same organization. As noted above, these results and the others generated by the conference must be treated with caution. They are important enough, however, to merit further study.

To that end, we propose convening at least three more conferences. One would focus on the tactical, strategic and organizational aspects of cyberterrorism. Bringing together hackers and individuals who can realistically play the roles of members of sub-state groups, it would explore further the utility of cyberterrorism and the issue of combining hackers and traditional practitioners in one organization. This conference would utilize a number of methods, including simulations on a closed computer system, to provide information on issues essential to understanding the possible future development of cyberterrorism. These issues include

- Technical details on information attack methodology
- An understanding of how hackers and practitioners separately would use information operations, including data on whether hackers prefer denial of service attacks or subversion of information systems and under what circumstances
- Information on the likelihood of cooperation between sub-state groups and hackers and on the likely ways practitioners might try to recruit hackers
- Information on how the integration of information technology and information technicians into sub-state groups might change their strategy, tactics and organization
- An understanding of the degree to which possessing effective information and communication technology decreases the importance of violence in sub-state conflict
- Information on the scale and scope of escalation when information operations are used (is mass disruption useful?) and the factors that influence decisions about the scale and scope of escalation

A second conference would convene representatives of groups with a religious motivation. These groups are often said to be more inclined to use extreme forms of violence and so would provide a further test of the hypotheses derived from the first conference about the likelihood of mass disruption and mass casualties. In addition, evidence suggests that some religious groups are among those most interested in using information technology. This should make them a priority subject for further analysis.

Finally, a third conference would collect a different set of practitioners from ethno-nationalist and revolutionary groups. This would allow us to further test and better substantiate the results of the first conference.

As part of this research effort, we will augment the work of the conferences by conducting interviews and field studies with individual hackers and terrorists.